

DDoS 防护

BGP 高防 IP

产品文档



腾讯云

【版权声明】

©2013-2018 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

BGP 高防 IP

产品介绍

产品概述

产品优势

购买指南

产品价格

计费说明

购买说明

使用须知

弹性防护

CC 防护

IP 封堵

回源 IP 段

转发流量

升级及续费

自动续费

告警信息

操作指南

使用教程

子账号告警信息

BGP 高防 IP

产品介绍

产品概述

最近更新时间：2018-06-14 15:25:43

什么是 BGP 高防 IP ？

BGP 高防 IP 是腾讯云面向所有用户推出的抗 DDoS 攻击的付费产品，支持任意源站位置，最高可达 900 Gbps 的 BGP 线路防护，能轻松有效应对 DDoS、CC 攻击，确保业务稳定正常。

适合哪些用户使用？

- BGP 高防 IP 适合所有用户接入，支持任意源站位置，支持所有业务类型。无论是腾讯云内、其他私有云或 IDC 机房的服务器，通过 BGP 高防 IP 均可实现防护的目的。
- 对网站类、非网站类业务有防护需求的用户。

产品原理是什么？

用户购买 BGP 高防 IP 且配置转发规则和域名回源后，此时所有的访问流量都将流经 BGP 高防 IP 集群，通过端口协议转发的方式（支持网站业务和非网站业务）将访问流量转发至源站，同时攻击流量将在 BGP 高防 IP 集群进行清洗和过滤，只会将正常业务流量返回至源站，从而确保源站业务的稳定。

为什么选择该产品？

- 隐藏真实源站 IP
通过将 BGP 高防 IP 作为业务 IP 对外发布的方式，隐藏用户真实源站 IP，让攻击流量无法直接到达源站，保护源站业务。
- 超大带宽防护
拥有业界最大 BGP 防护带宽，最高可达 900 Gbps + 防护，轻松抵御 DDoS、CC 攻击。
- 优质访问体验
采用 BGP 防护带宽，多达 30 线的 BGP 线路，带来极速访问体验。

- 灵活计费

支持“保底防护 + 弹性防护”模式，按实际攻击量计费，为用户节约成本。详情可参考 [弹性防护](#)。

使用时需要注意什么？

BGP 高防 IP 是通过将高防 IP 作为业务 IP 对外发布来隐藏源站 IP 的方式实现防护目的，若用户源站曾被攻击过且源站 IP 已暴露，那么建议购买 BGP 高防 IP 服务后更换源站 IP，以确保源站 IP 的隐秘性，让攻击者无法直接攻击源站。

产品优势

最近更新时间：2018-06-06 09:39:20

BGP 高防 IP 是腾讯云面向所有用户推出的抗 DDoS 攻击的付费产品，支持任意源站位置，其产品优势如下：

无源站限制，轻松接入

无论是在腾讯云、其他私有云或 IDC 机房的服务器，通过 BGP 高防 IP 均可实现防护的目的。

隐藏源站 IP

通过将高防 IP 作为业务 IP 对外发布，隐藏客户真实源站 IP，让攻击流量无法直达源站，进一步保证源站安全。

30 线的 BGP 线路

采用 BGP 防护带宽，单 IP 对接多线路，线路可靠且覆盖面广。同时，平均访问时延小于 30 ms，消除跨网访问时延，带来优质访问体验。

超大带宽防护

拥有单点 T 级超大防护带宽，对单客户单点可提供 300 Gbps + BGP 防护及 900 Gbps + 单线防护能力，轻松抵御大流量 DDoS 攻击。

领先清洗能力

自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，有效防御各类攻击。

多业务支持

支持 TCP / UDP 协议，可全面防护网站和非网站类业务，全行业均有最佳实践和解决方案。

弹性防护，灵活付费

当攻击流量超过套餐峰值时，腾讯云仍为客户继续防护，保障业务不中断。按当天实际攻击量付费。

购买指南

产品价格

最近更新时间：2018-11-26 17:34:21

保底防护（按月预付费）

DDoS 防护	CC 防护	大陆 BGP（元/月）	境外 BGP（元/月）
10Gbps	20,000QPS	-	20,000
20Gbps	40,000QPS	6,000	30,000
30Gbps	70,000QPS	16,600	47,000
40Gbps	100,000QPS	-	55,000
50Gbps	150,000QPS	25,600	67,000
60Gbps	200,000QPS	-	80,000
80Gbps	250,000QPS	-	90,000
100Gbps	300,000QPS	80,600	96,000

① 说明：

- 对于大陆地区的非腾讯云上用户，购买保底套餐默认赠送100M转发带宽。
- 可提供 T 级防护能力，如有需要，请联系您的商务经理进行定制。

弹性防护（按天后付费）

- 弹性防护可免费开启。未触发弹性防护，不产生费用。
- 当触发弹性防护（攻击峰值超过保底防护峰值）时，取当天实际发生的最高攻击峰值所对应计费区间进行计费，账单次日生成。

⚠ 注意：

弹性防护峰值为最高防护峰值，如果弹性防护峰值与保底防护带峰值一样，则不会产生后付费且最高防护峰值为保底防护带峰值。

DDoS 防护峰值	大陆 BGP (元/天)	境外 BGP (元/天)
0Gbps < 攻击峰值 ≤ 10Gbps	-	1,000
10Gbps < 攻击峰值 ≤ 20Gbps	-	2,200
20Gbps < 攻击峰值 ≤ 30Gbps	3,500	2,800
30Gbps < 攻击峰值 ≤ 40Gbps	4,800	4,800
40Gbps < 攻击峰值 ≤ 50Gbps	5,700	5,700
50Gbps < 攻击峰值 ≤ 60Gbps	6,600	8,000
60Gbps < 攻击峰值 ≤ 70Gbps	7,500	12,000
70Gbps < 攻击峰值 ≤ 80Gbps	8,350	15,000
80Gbps < 攻击峰值 ≤ 90Gbps	9,200	17,000
90Gbps < 攻击峰值 ≤ 100Gbps	10,050	18,000
100Gbps < 攻击峰值 ≤ 120Gbps	11,750	20,000
120Gbps < 攻击峰值 ≤ 150Gbps	14,300	22,000
150Gbps < 攻击峰值 ≤ 200Gbps	18,550	27,000
200Gbps < 攻击峰值 ≤ 250Gbps	22,800	36,000
250Gbps < 攻击峰值 ≤ 300Gbps	26,800	40,000
300Gbps < 攻击峰值 ≤ 400Gbps	-	48,000

转发流量

按转发带宽预付费，具体价格请参考如下表格：

带宽	大陆价格 (元/月)	境外价格 (元/月)
50Mbps	-	4,500

带宽	大陆价格 (元/月)	境外价格 (元/月)
100Mbps	0 (默认赠送)	9,000
150Mbps	4500	13,500
200Mbps	9000	18,000
500Mbps	36000	45,000
1Gbps	81000	90,000
2Gbps	171,000	180,000

计费说明

最近更新时间：2018-06-06 10:01:41

计费规则

计费项	保底防护峰值	弹性防护	转发流量	
计费模式	包年包月	按天按量计费	包年包月按带宽计费	按天按量计费
付费方式	预付费	后付费	预付费	后付费
付费说明	购买时一次性支付 若升级保底防护，则在原有的基础上加收额外费用	弹性防护可免费开启 触发弹性防护后，取当天弹性防护峰值按区间收费，账单次日生成 若未触发弹性防护则不收取任何费用	购买时选择转发带宽大小 一次性支付	购买时选择按转发流量计费，收费标准为 0.80 元 / GB 后付费，账单次日生成

到期预警

BGP 高防 IP 服务会在到期前的第 7 天，通过 **站内信、短信及邮件** 的方式向您推送到期预警消息。

升级和续费

- 若您升级保底防护，则加收额外的升级费用，且防护只可升级，不可降级。
- 账户余额充足的情况下，若您已设置自动续费，系统在到期当日会自动续费。

回收机制

服务到期后，系统仍为您提供 5 天的服务且暂时保留配置。若 5 天内未续费，则 BGP 高防 IP 将自动销毁，服务停止。

购买说明

最近更新时间：2018-12-06 15:02:08

购买地区

BGP 高防 IP 可绑定任意云内外设备，考虑到时延，推荐选择近源高防。开放购买的地域包括：

- 中国大陆：华南地区（广州）、华东地区（上海）、华北地区（北京）。
- 国际区域：港澳台地区（中国香港）、亚太地区（新加坡、首尔、曼谷、印度、东京）、美国西部（硅谷）、美国东部（弗吉尼亚）、北美地区（多伦多）、欧洲地区（莫斯科、法兰克福）。

用户可在各地直接在线购买的高防服务如下：

地区	保底防护	弹性防护	最大防护能力
广州	20 - 50Gbps	30 - 100Gbps	100Gbps
北京	20 - 50Gbps	30 - 100Gbps	100Gbps
上海	20 - 100Gbps	30 - 300Gbps	300Gbps
境外	10 - 100Gbps	30 - 400Gbps	400Gbps

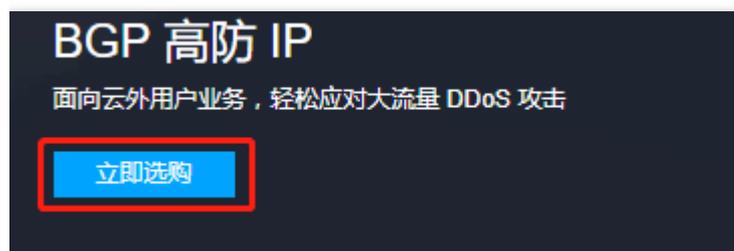
⚠ 注意：

本产品可定制 T 级防护能力，如有需要，请联系您的商务经理进行定制。

购买方式

介绍页购买

在腾讯云官网，从 [DDoS 防护](#) 页面中进入 [BGP 高防 IP](#) 产品介绍页，单击【立即选购】进行购买。



控制台购买

1. 登录 [BGP 高防 IP 控制台](#)，进入【资产列表】页面，单击【新建】。



2. 选择防护配置，选择购买数量及购买时长。

地域：BGP 高防 IP 提供代理转发方式，请尽量选择靠近源站服务器位置的地域，减少访问时延。目前 BGP 高防 IP 不仅适用于业务服务器部署在中国大陆地域内的 DDoS 防护场景，同时支持中国大陆以外的地域。

保底防护峰值：为包年包月预付费。建议以历史攻击流量的平均值为参考，选择的保底防护峰值略高于平均值，以便足够防御大部分攻击行为。

弹性防护峰值：为按实际防护量计费，每日结算。建议以历史最高攻击流量为参考，选择的弹性防护峰值略高于历史最高峰值，以便发生大流量攻击时有足够的容量可以防御，避免超过防护峰值 IP 被封堵。

转发带宽：为经过 BGP 高防专区转发到源站服务器的业务流量，建议根据正常业务流量特点选择带宽。

自动续费：用户可自行勾选，当账户余额充足情况下，服务到期后将按月自动续费，保障业务防护不中断。

BGP高防IP

BGP高防IP限时特惠，包年包月预付费6个月及以上88折，1年83折，2年7折，3年5折。BGP高防IP简介 [查看](#)

业务部署在 腾讯云公有云 腾讯金融云 非腾讯云 [详细对比](#)

地域 华南地区 华东地区 华北地区 港澳台地区 亚太地区

广州	上海	北京	香港	新加坡	曼谷	印度	首尔
亚太地区		美西地区		欧洲地区		北美地区	
东京	硅谷	莫斯科	法兰克福	弗吉尼亚	多伦多	详细对比	

建议华南及西南地区客户选用

保底防护峰值 20Gbps 30Gbps 50Gbps

CC防护峰值 40,000QPS

弹性防护峰值 无 30Gbps 40Gbps 50Gbps 60Gbps 70Gbps 80Gbps 90Gbps 100Gbps [了解详情](#)

骨干线路故障等不确定因素，可能造成弹性防护失败。若未达到弹性上限发生封禁，免除当日弹性防护费用
为保障您的业务稳定运行，建议您开启弹性防护

转发带宽 100Mbps 150Mbps 200Mbps 500Mbps 1Gbps 2Gbps

HTTP : 3000QPS
HTTPS : 3000QPS
如果规格无法满足需求，请联系腾讯云售后定制。

购买个数 - 1 + (一次最多购买1个)

购买时长 1个月 2个月 3个月 半年 1年 2年 3年 [其他时长](#)

自动续费 账户余额足够时，设备到期后按月自动续费

根据国家监管要求，所有使用高防业务的域名必须经过ICP备案，未备案域名将无法访问， [备案入口](#)

3. 单击【立即支付】完成支付流程。

使用须知

弹性防护

最近更新时间：2018-10-18 11:13:24

弹性防护有什么作用？

开启弹性防护后，当攻击流量超过购买的保底防护峰值且在弹性防护范围内时，腾讯云 BGP 高防包可继续为您提供防护，保障业务访问持续性。

注意：

弹性防护峰值不能小于保底防护峰值。若您选择的弹性防护峰值等于保底防护峰值，则相当于弹性防护能力不生效。

如何计算防护峰值？

- 如果未开启弹性防护，则保底防护峰值为高防 IP 实例的最高防护峰值。
- 如果开启了弹性防护，则弹性防护峰值为高防 IP 实例的最高防护峰值。

例如，您购买了 20Gbps 的保底防护，同时开启 50Gbps 的弹性防护，则最高的防护能力是 50Gbps。

注意：

您可根据自身业务需求，随时调整弹性防护值。

弹性防护如何收费？

弹性防护可自主开启。只有当攻击流量超过保底防护峰值，即触发弹性防护后，才收取费用，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。

例如：您购买 20Gbps 的保底防护，且设置了 50Gbps 的弹性防护，当天发生实际攻击峰值为 35Gbps，我们将收取 30Gbps - 40Gbps 区间的弹性防护费用。

详细费用请参见 [产品价格](#)。

CC 防护

最近更新时间：2018-12-14 18:43:32

什么是 CC 攻击？

CC 攻击即 ChallengeCollapsar 攻击，指攻击者借助代理服务器生成指向受害主机的合法请求，拥塞被攻击方的网络和服务器性能，实现攻击目的。

什么是 CC 防护？

CC 防护即指针对 CC 攻击的防护。

如何开启 CC 防护？

特别提醒：

CC 防护可根据您自身业务情况选择开启。

1. 登录 [DDoS 防护（大禹）](#) 控制台，在“BGP 高防 IP”控制页中找到您所购买的 BGP 高防 IP 实例；



2. 选择所要开启 CC 防护的 BGP 高防 IP 实例，单击实例名称进入 BGP 高防 IP 详情页面；

高防IP

华南地区(广州) ▾ BGP ▾

您已使用BGP高防IP 天，累计为您抵御DDoS攻击 次。

[新建](#)

ID/名称	高防IP	转发规则数
bgpip 未命名		4

3. 在 CC 防护一栏开启 CC 防护开关，根据自身业务需要设置 HTTP 请求阈值即可，推荐您将 HTTP 请求阈值设置为业务量的 1.2 倍。

CC防护

CC防护 对于敏感业务，可将业务URL添加到URL白名单，对该业务不做CC攻击检测和防护

http请求数阈值 当http请求数超过设定值时，触发CC防护。

IP 封堵

最近更新时间：2018-12-14 18:45:08

什么是 IP 封堵？

IP 封堵指在访问您域名的流量通过腾讯云清洗集群时，会将您的所有流量指向 NULL（即通常所说的黑洞路由，也可以理解为丢弃流量）。若被封堵，业务将不可访问。

怎样会被封堵？

- 当您的 IP 受到攻击，且达到了防护峰值（弹性防护峰值）时，就会触发 IP 封堵，普通情况下封堵时长为 2 小时，大流量攻击封堵时长为 24 - 72 小时。
- 若平台同时遭受多方攻击，为了保障平台稳定性，将会触发运营商封堵，您的业务也将无法访问；此时若未达防护峰值，将免收相关弹性防护费用，运营商封堵默认在 24 小时后解除。

封堵告警

- 当您的 IP 遭攻击且被封堵时，我们将通过站内信、短信及邮件的方式向您推送封堵告警消息。
- 若想了解更多告警信息相关内容，请参见 [告警信息](#)。

提前解封

如需提前解封，您可以升级 BGP 高防产品：

已购买 BGP 高防 IP 产品的用户，建议您 [升级](#) 保底防护，以提前解封高防 IP。

注意：

开启 [弹性防护](#)，可帮您抵御大规模流量攻击，且弹性防护按天按量灵活付费，可节约您的成本。您可参见 [使用教程](#) 中的 [开启防护](#) 相关内容来开启弹性防护。

回源 IP 段

最近更新时间：2018-09-14 15:31:19

什么是回源 IP？

回源 IP 指 BGP 高防 IP 集群将业务流量转发至您源站时所用的 IP。

为何要放行回源 IP 段？

当您使用 BGP 高防 IP 服务后，您所有的业务流量首先会流经 BGP 高防 IP 集群，集群会将清洗后的业务流量转发至您的源站。为了防止您将高防回源 IP 拦截或限速导致业务流量受损，您需将 BGP 高防 IP 回源 IP 段添加至您源站的防火墙或者其他主机安全防护软件的白名单中。

转发流量

最近更新时间：2018-11-26 17:34:13

什么是转发流量？

转发流量指的是 BGP 高防 IP 集群转发到用户源站的流量。

转发流量如何收费？

转发流量按包年包月的转发带宽计费方式，一次性付费。详细价格请参见 [产品价格](#)。

⚠ 注意：

对于大陆地区的云外用户，购买保底套餐默认赠送10Mbps转发带宽。若发现不够用时，请及时升级业务带宽，以免业务访问体验受到影响。

升级及续费

最近更新时间：2018-12-14 18:46:41

登录控制台

登录 [BGP 高防 IP 控制台](#)，在控制页中找到您所购买的 BGP 高防 IP 实例。

大禹网络安全

基础防护

BGP高防包

BGP高防IP

棋牌盾

高防IP 华南地区(广州) ▾ BGP ▾

您已使用BGP高防IP 天，累计为您抵御DDoS攻击 次。

新建

ID/名称	高防IP	转发规则数
-------	------	-------

升级或续费

您可以根据自身的需求，选择【升级】或【续费】。

高防IP 华南地区(广州) ▾ BGP ▾

您已使用BGP高防IP 天，累计为您抵御DDoS攻击 次。

新建

Q

1. 升级

单击【升级】后，在“升级”控制界面中选择您需要的“升级保底防护值”，单击【立即升级】即可。

升级



ID/名称 bgpip- [redacted] IDC-probe-by-George

高防IP [redacted]

当前保底防护
峰值 10 Gbps

过期时间 2019-03-07 11:25:26

升级保底防护

10 Gbps 20 Gbps 30 Gbps 40 Gbps 50 Gbps

cc防护峰值：40,000QPS

升级费用 **76,147.72元**

立即升级

取消

2. 续费

单击【续费】后，在“续费”控制界面中选择您需要的“续费时长”，单击【立即续费】即可。

续费 ×

ID/名称 bgpip- [redacted] IDC-probe-by-George

高防IP [redacted]

当前保底带宽 10 Gbps

峰值

续费时长

1月	2月	3月	4月	5月	6月 促	7月 促	8月 促	9月 促	1年 促	2年 促	3年 促
----	----	----	----	----	------	------	------	------	------	------	------

有效期至 2019-04-07 11:25:26

总计费用 **8,600.00元**

立即续费 取消

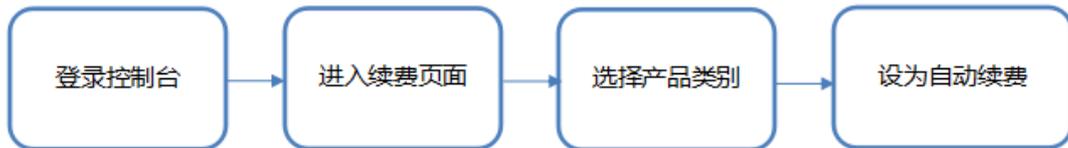
注意：

保底防护峰值只可提高不可降低，若您需要超大防护能力来保证业务正常可开启 [弹性防护](#)。

自动续费

最近更新时间：2018-12-14 18:47:24

BGP 高防 IP 设置为自动续费的具体操作流程图如下：



登录控制台

登录 [BGP 高防 IP 控制台](#)；

The screenshot shows the Tencent Cloud console interface. The top navigation bar includes '总览' (Overview), '云产品' (Cloud Products), '云服务器' (Cloud Servers), '域名服务' (Domain Services), and '网站备案' (Website Filing). The '大禹网络安全' (Da Yu Network Security) menu item is highlighted with a red box. Below it, the '基础防护' (Basic Protection) sub-menu is selected. The main content area displays 'DDoS基础防护' (DDoS Basic Protection) with a table of instances.

主机名	绑定
bghostzhu测试机	203

进入续费页面

在右上角选择【费用】>【续费】；



选择产品类别

在产品类别中选择【BGP 高防 IP】；



设为自动续费

勾选对应的 BGP 高防 IP，在手动续费项中，单击【设为自动续费】即可。

手动续费项(6)	自动续费项(0)	到期不续费(0)	
批量续费	设为自动续费	决定不续	统一到期日
<input type="checkbox"/>	待续费项		
<input checked="" type="checkbox"/>	BGP高防IP : [模糊]	ID : bgpip-[模糊] . ip : [模糊]	

告警信息

最近更新时间：2018-06-06 09:45:14

什么情况下会收到告警信息？

当用户所使用的 BGP 高防 IP 受到攻击、受攻击结束、IP 被封堵、解除封堵时，均会收到告警信息提示：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后 15 分钟，您将收到攻击结束提示。
- IP 封堵被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

告警信息是以什么形式进行推送？

告警信息将通过站内信、短信及邮件的方式向您推送。

拥有多个子账号时，子账号都会收到告警信息吗？

子账号只要设置了对应的短信和邮件地址，子账号就可以收到告警信息。

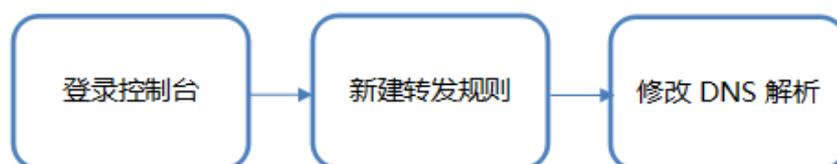
如何设置子账号接受主账号的告警信息，请参见 [子账号告警信息](#)。

操作指南 使用教程

最近更新时间：2018-12-14 18:47:41

业务部署在非腾讯云

BGP 高防 IP 使用流程如下图所示：



登录控制台

1. 登录 [DDoS 防护 \(大禹\)](#) 控制台。



2. 在“BGP 高防 IP”控制页中找到您已经开通的业务部署在非腾讯云的高防 IP 实例。

高防IP 华南地区(广州) BGP

您已使用BGP高防IP 天，累计为您抵御DDoS攻击 次。

新建

ID/名称	高防IP	转发规则数	转发目标
bgp 未命名		4	非腾讯云
		5	非腾讯云

3. 单击实例 ID，进入配置页面。

ID/名称	高防IP	转发规则数	转发目标
bgpip 未命名		4	非腾讯云
bgpip-		5	非腾讯云

新建转发规则

1. 在“转发规则”配置栏中，单击【新建】按钮，新建转发规则。

转发规则

新建 每个高防IP支持60条转发规则，每条规则支持20个源站IP。

转发协议/端口	源站端口	源站IP
		没有记录

2. 添加转发规则操作按下图所示，转发协议支持 TCP 协议，填写转发端口（即最终用于访问高防 IP 端口，一般与源站端口相同）、填写源站端口（源站提供服务的真实端口）和源站 IP，单击【确定】后会生成一条转发规则。

添加转发规则

转发协议

转发端口

源站端口

源站IP

请用回车分隔多个IP，最多可输入本IP转发目标区域内20个公网IP

注意：

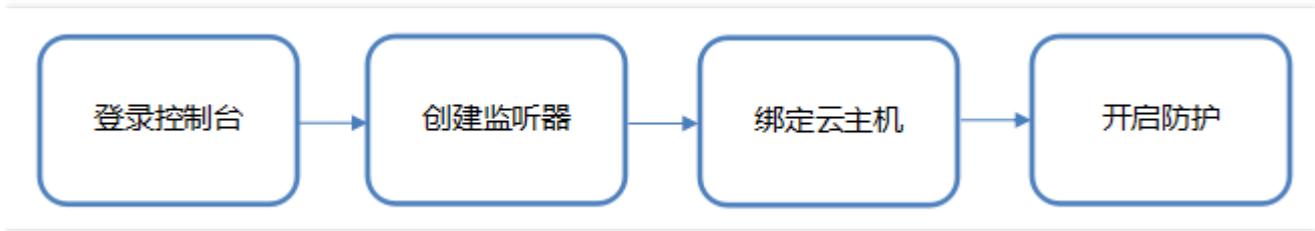
- 请用回车分隔多个 IP，最多可输入本 IP 转发目标区域内 20 个公网 IP。
- 配置多个源站 IP 时，会以源 IP 哈希方式进行负载均衡。
- 一个高防 IP 支持配置 60 条转发规则。

修改 DNS 解析

最后将 A 记录指向的 IP 地址修改为 BGP 高防 IP 即可。

业务部署在腾讯云

BGP 高防 IP 使用流程如下图所示：



登录控制台

1. 登录 [DDoS 防护 \(大禹\)](#) 控制台；



2. 在 “ BGP 高防 IP ” 控制页中找到您已经开通的业务部署在腾讯云的高防 IP 实例，单击实例 ID，进入配置页面。

BGP高防IP 华南地区(广州) ▾

您已使用BGP高防IP 144 天，累计为您抵御DDoS攻击 0 次。

[新建](#)

ID/名称	高防IP	转发规则数	转发目标	防护峰值 ↓	超峰次数 ↓
未命名	[模糊]	0	腾讯公有云	20 Gbps	0
tesbx	[模糊]	0	腾讯公有云	10 Gbps	0

创建监听器

1. 基本配置根据业务情况设置相应的协议端口，高防 IP 是四层转发，七层应用协议，如 HTTP 等也是选择 TCP ，如下图：

创建监听器 ✕

① 基本配置 >
② 高级配置 >
③ 健康检查

名称

监听协议端口

后端端口

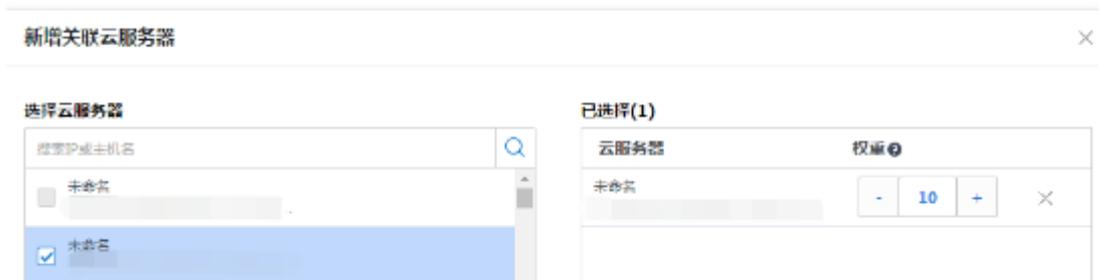
2. 高级配置可以根据业务具体情况配置，如不清楚，默认配置即可。



3. 健康检查默认是开启，建议不要自行修改配置，这里可以对出故障的服务器端口进行自动踢除，保障业务可用。

绑定云服务器

绑定云服务器，设置权重即可。



开启防护

开启相应防护，可以设置弹性防护峰值，并开启 CC 防护,并设置阈值。

< BGP高防IP | bgpip-000000q5

弹性防护

当前状态	已开启	关闭
弹性峰值	10Gbps	更改

CC防护

CC防护 对于敏感业务 可将业务URL添加到 [URL白名单](#)，对该业

http请求数阈值 当http请求数超过设定值时，触发CC防

监听器

[+ 新建](#)

监听器名称	操作
> 123(TCP:80)	修改 删除

子账号告警信息

最近更新时间：2018-12-14 18:48:28

腾讯云DDoS防护（大禹）BGP高防IP在您所使用的BGP高防IP受到攻击、受攻击结束、IP被封堵、解除封堵时，都会为您推送告警信息。

下面将为您介绍设置子账号接受主账号告警信息的详细操作。

1. 登录您的腾讯云账号，进入 [消息中心](#)，或者通过 [用户控制台](#)，单击右上角消息按钮，在单击弹出页面底部的【进入消息中心】；

The screenshot shows the Tencent Cloud console interface. At the top right, a notification bell icon is highlighted with a red box. Below it, the '消息中心' (Message Center) panel is open, displaying '暂无未读消息' (No unread messages). The left sidebar contains navigation menus for '视频服务' (Video Services), '金融服务' (Financial Services), '区块链' (Blockchain), and '人工智能 (AI)' (Artificial Intelligence). The middle section shows '余额 -' (Balance -), '最新公告' (Latest Announcements), and '待办事项' (To-do Items) with buttons for '异常对象数', '待支付订单', '待续费项 (30)', and '待处理工单数'. At the bottom right of the message center, a button labeled '进入消息中心' (Enter Message Center) is highlighted with a red box.

2. 单击左侧目录中的【消息订阅】进入消息列表；



3. 在消息列表中，找到“安全消息通知”，单击右侧的【编辑】，进入编辑页面；

<input type="checkbox"/>	产品服务相关通知	✔	✔	✔	文档测试帐号	编辑
<input type="checkbox"/>	渠道服务通知	✔	✔	✔	文档测试帐号	编辑
<input type="checkbox"/>	安全消息					收起
<input type="checkbox"/>	安全事件通知	✔	✔	✔	文档测试帐号	编辑
<input type="checkbox"/>	内容违规通知		✔	✔	文档测试帐号	编辑
<input type="checkbox"/>	腾讯云动态					收起
<input type="checkbox"/>	云+社区相关通知			✔	文档测试帐号	编辑
<input type="checkbox"/>	活动通知	✔	✔	✔	文档测试帐号	编辑

4. 选择接收人和接收方式之后，单击【确定】即可。

设置接收人和接收方式

要添加或修改用户和用户组的信息可以前往 [用户与权限](#)

消息类型 **安全事件通知**

接收人

用户	用户组
<input checked="" type="checkbox"/> 文档测	
<input type="checkbox"/> 协	!
<input type="checkbox"/> 消息	!
<input type="checkbox"/> sut	
<input type="checkbox"/> 125	

已选 1 人

文档测

接收方式 站内信 邮件 短信 微信